Return

Project Tracking No.: P-007-FY06-DHS

Return on Investment (ROI) Program Funding Application

This template was built using the ITD ROI Submission Intranet application.
FINAL AUDIT REQUIRED: The Enterprise Quality Assurance Office of the Information Technology Department is required to perform post implementation outcome audits for all Pooled Technology funded projects and may perform audits on other projects.

This is a Pooled Technology Fund Request. Amount of funding requested: $750,000.00

Section I: Proposal

Date:	7/14/2004
Agency Name:	DHS - Administration
Project Name:	DHS HIPAA SECURITY AND IT STRATEGY DIRECTION
Agency Manager:	Delno Wadle
Agency Manager Phone Number / E-Mail:	(515)281-5609 / dwadle@dhs.state.ia.us
Executive Sponsor (Agency Director or Designee):	Steve Mosena

A. Project Summary

Describe the nature and use of the proposed project, including what is to be accomplished, how it will be accomplished, and what the costs and benefits will be.
Response:

The focus of DHS's efforts since 2000 when a HIPAA assessment was performed encompasses not only electronic standard transactions (now successfully complete) but Privacy and Security dimensions for the Department as a whole. With the advent of several pieces of legislation sighted in section D. below it is apparent to the DHS CIO and Security Officer that more progressive and imposing legislation is in the offing. Further, the Security dimension for an enterprise the size of DHS is a huge undertaking with far reaching impact on all systems, personnel and operations. In addition to the legislation, organizations and software companies are adopting and aligning established best practices methodologies with legislative and organizational requirements. DHS has watched the progressive nature and building momentum of both legislation and best practices, which really are at the root of all the described efforts though methodologies may vary. But all serve as a structured approach to business practices. Particulars will be delineated below. The Data Management Division of DHS voluntarily requested an the following audits by the Gartner Group (at a cost of $166,00.00)– 1.Rapid Assessment for IT Overview Analysis 2.Organizational Readiness Assessment 3.Organizational Readiness and Technology Assessment, Skills Inventory and Assessment of Current Technology. While the findings show many strengths, the posture it blueprints points to some very real dangers for an entity serving hundreds of thousands of Iowans which must be addressed as we go forward. This study was completed in March of 2004. The DHS CIO has envisioned, unveiled and has approval for a complete change in DHS strategic vision, named "IT Strategy Direction" which will be outlined below. Consider for a moment that DHS is responsible for benefit administration of $2,775,613,346. Lastly, a very subtle point that is not well understood for Security practices embedded in all the referenced legislation is not just confidentiality / privacy but the two elements of availability and integrity which have far reaching implications on business requirements. One major impact is Business Continuity Planning (BCP) (and Implementation and Maintenance).

B. Strategic Plan

How does the proposed project fit into the strategic plan of the requesting agency?
Response:

As indicated above our CIO is developing a strategic plan in Fiscal ’05 reflecting an Enterprise Strategic Plan (IT Strategy Direction) which will revolutionize DHS’s approach and encompasses the following guidelines – 1.Develop and maintain a Technology Strategic Plan to support the Department’s business vision. 2.Anchor strategic planning in customer needs. 3.Develop and promote long term and mid range planning that establishes clear linkages between the Department’s Strategic Plan, its business processes, it’s performance measures and the state’s Information Technology Strategic Plan. 4.Implement a comprehensive System Life Cycle methodology. 5.Bridge the current and future organizational requirements with quality IT solutions and direction from the Division of Data Management. 6.Treat technology projects as investments through the use of Information Technology Investment Management (ITIM). The department is undertaking a pilot program in ’05 the implement Information Technology Investment Management (ITIM) and Information Technology Information Library-Information Technology Service Management (ITIL-ITSM). This pilot program will serve as an enterprise model for the department and potentially the state enterprise. This effort aligns with the State of Iowa Information Technology Strategic Plan particularly the Assumptions. As outlined below in C. the department has expended very substantial resources during Fiscal 04 in setting the direction for continuing work over the next several years, all rooted in HIPAA starting back in 2000. The Gartner findings indicates the following weaknesses which must be and will be addressed with new strategic direction. 1.Under-investment in IT infrastructure 2.Under-investment in applications systems 3.Under-investment in organization and staffing 4.Difficulty in prioritizing project that go across departments and agencies. 5.Need to improve Midrange Computing 6.Need to improve Distributed Computing 7.Need to monitor wide area data network by tracking service levels and customer satisfaction. 8.Need to focus on improving flexibility, data analysis capabilities, and integration. 9.Define new organization structure to improve efficiency and effectiveness 10.Improve workforce management. 11.Improve overall DHS governance.

C. Current Technology

Provide a summary of the technology used by the current system. How does the proposed project impact the agency's technological direction?
Response:

1) Software (Client Side / Server Side / Mid-Range / Mainframe) : DHS has a user community numbering some 5,800 users/workers in over 150 locations supported by over 220 network servers. a) Application Software It should be noted that during fiscal ’04 DHS invested heavily (approx $600,000.00) in a new suite of security tools and information repository, namely, 1. Symantec Enterprise Security Manager, 2. sophisticated Storage Tech backup capabilities and a backup unit at the Stark Armory, 3.Tumbleweed filtering and encryption software, 4. Symantec Vulnerabiltiy suite – NetRec and Magic Enterprise Software suite for helpdesk, service desk, incident tracking and escalation. This latter tool will be enhanced during ’05 to begin identifying and piloting an enterprise Information Technology Service Management model. It is this new suite of tools which is being put under a Capability Maturation Model (CMM) as the backbone for DHS Security and service improvement. Magic Enterprise Software was ITIL Certified over 14 years ago. DHS uses a variety of software, some off-the shelf such as Microsoft Office Suite with others coded internally on both mainframe and client server architecture. The 80 mainframe systems and 110 SQL based (Client Server/ Web) systems have been developed in a variety of programming environments. Some of those include: COBOL, JCL, CICS, IDMS, SQL, FLASH, and Visual Basic, HTML, VBSCRIPT. There internal systems interface with each other and data from several of the systems is shared with other agencies, e.g. DOC, IWD, DPH, DEPT ED. b) Operating system software Win 95 AND Win2000 Desktop, NT 4.0, Win2000 Server, Z/OS 1.4 mainframe, SQL 6.5 & 7.0 and 2000. c) Major interfaces to other systems, both internal and external 8 major systems in the department with interfaces and data exchange with each other and with other agencies, e.g. DOC, IWD, DPH, Dept Ed. The DHS estimate of just reports generated exceed 8,000. It must be noted that the Gartner report referenced elsewhere shows the definitive and critical need to re-engineer, replace 6 major mainframe applications (described as underfunded, complex and antiquated) because existing infrastructure CANNOT SUPPORT FUTURE BUSINESS OBJECTIVES. In addition, with the advent of the new Iowa Medicaid Enterprise (IME), it brings another huge renovation requirement bringing to 6 major application re-engineering efforts.

D. Statutory or Other Requirements

Is this project or expenditure necessary for compliance with a Federal law, rule, or order?
☑ YES (If "Yes", cite the specific Federal law, rule or order, with a short explanation of how this project is impacted by it.)
Explanation:
Health Insurance Portability and Accountability Act of 1996 (HIPAA) {public law 104-191} 104 Congress.

We must keep in mind that HIPAA was preceded by the FEDERAL INFORMATON SECRUITY MANAGEMENT ACT AND FOLLOWED BY THE SARBANES-OXLEY ACT. In the aftermath of 9/11 Federal Homeland and State Homeland Security agencies arose. The resulting National Cyber Space Strategy (Feb 2003 report) along with State Governors Cyber Security Task Force have studied Security needs analyzed have been compiled into the Information Security Governance – A Call to Action (report of April 2004).

All of these reports talk to methodologies such as "IDEAL" (Initiating, Diagnosing, Establishing, Acting, Learning), ITIL-ITSM (Information Technology Information Library-Information Technology Service Management).
ITIL Service Management, a model and methodology adopted by the UK over 14 years ago focuses on 2 major components
1.Service Delivery Set
a.Service Level Management
b.Financial Management
c.Capacity Management
d.Availability Management
2.Service Support Set
a.Incident Management
b.Problem Management
c.Configuration Management
d.Change Management
e.Release Management

The ISO/IEC 1799 Specifications, specifications – models from NIST, Carnegie Mellon, SEI, BCI.org, ITIL and others ultimately aspire to the concept of best practices and continuous process improvement, alignment of IT to Business needs. All of these organizations are pioneers in business and concept security models and urge business and government to freely use the results of their efforts.

Is this project or expenditure required by state law, rule or order?
☑ YES (If "YES", cite the specific state law, rule or order, with a short explanation of how this project is impacted by it.)
Explanation:
While Information Security Governance- A Call to Action, Homeland Security Efforts, Governors Cyber Space Task Force have not yet mandated by law requirements they certainly are URGING adoption of and

alignment with very specific methodologies focusing on continuous process improvement and business continuity. This is the trend that DHS has been observing and we consider our vision and continuing effort to be well ahead of the average organization. But large resources requirements are needed to pursue the vision.

Does this project or expenditure meet a health, safety or security requirement?

☑ YES (If "YES", explain.)

Explanation:

Health -- The Federal HIPAA law requires compliance to meet national standards involving the electronic transmission of health data. Through standardized electronic formats, communications are greatly simplified between state agencies, fiscal agents, federal government and providers.

Safety -- Compliance insures that state agencies and private sector partners have access only to the health related information minimally to conduct core business functions while protecting the privacy and security of the clients we serve. Additionally the number of clients served and the billions of dollars administered obligates us to implement a large security net described below.

Security -- Compliance not only requires safeguarding medical data of the clients we serve but must insure Confidentiality, Integrity and Availability which increases the scope of effort to encompass Best Practices of service management from service support, to service delivery, to emergency operations, disaster recovery, business continuity and continuous process improvement.

Is this project or expenditure necessary for compliance with an enterprise technology standard?

☑ YES (If "YES", cite the specific standard.)

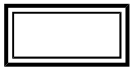
Explanation:

DHS has been in the development and implementation phase of far reaching Security Standards required by HIPAA and departmental requirements and other best practices being adopted by the Department for the last 13 months and continuing into ’05 for process development, testing and validation.
DHS efforts align with the State of Iowa Information Technology Strategic Plan. DHS is adopting an entirely new IT Strategy Direction described herein, aligns with Information Security Governance – A Call to Action, and numerous think-tank best practices approaches. We are confident that our approach will serve as a catalyst and model for the DHS ENTERPRISE and very well for the State Enterprise. Much of that content is described herein.
The Security requirements are Confidentiality, Integrity, and Availability with far reaching implications for both mainframe and Client Server / Web based applications with even greater impact on Network requirements.

[This section to be scored by application evaluator.]

Evaluation (20 Points Maximum)

If the answer to these criteria is "no," the point value is zero (0). Depending upon how directly a qualifying project or expenditure may relate to a particular requirement (federal mandate, state mandate, health-safety-security issue, or compliance with an enterprise technology standard), or satisfies more than one requirement (e.g. it is mandated by state and federal law and fulfills a health and safety mandate), 1-20 points awarded.



E. Impact on Iowa's Citizens

a. Project Participants

List the project participants (i.e. single agency, multiple agencies, State government enterprise, citizens, associations, or businesses, other levels of government, etc.) and provide commentary concerning the nature of participant involvement. Be sure to specify who and how many **direct** users the system will impact. Also specify whether the system will be of use to other interested parties: who they may be, how many people are estimated, and how they will use the system.

Response:

The following resources will have input into the development of all projects:
-- Department of Human Services policy staff : Provides policy expertise in the gap analysis phase and assistance with components of HIPAA implementation (5-10).
-- Department of Human Services Data Management staff: Implement modifications to internal enrollment systems and Title 19 files as required by HIPAA (7-10).
-- Department of Human Services line staff: Provide input on privacy and security related issues (15-20).
-- Department of Human Service management staff: Acts as HIPAA Steering Committee to ensure successful implementation (2-5).
-- Clients: Provide input in response to privacy and security components of HIPAA.
-- Providers/Provider Associations: Interface with the DHS staff to ensure smooth transition of business processes between entities (5).
-- Medicaid Fiscal Agent: Conduct requirements analyses, assist with communication to external entities, and modify Medicaid Management Information System (7).

All non-Medicaid systems as RTS, POS, FACS, State Payment system, Hawk-I and others which may surface through a gap assessment (10).
--Information Technology Department staff: Assist with the security component of HIPAA (2).
--Attorney General: Provide interpretation of the HIPAA regulations and guidance on implementation strategies (2).
--The new DAS Information Security Office (2).
--The 8 DHS facilities and mental health resources as well as 150 office locations around the state are the front lines
of our services to the citizens of Iowa (25).

b. Service Improvements

Summarize the extent to which the project or expenditure improves service to Iowa citizens or within State government. Included would be such items as improving the quality of life, reducing the government hassle factor, providing enhanced services, improving work processes, etc.
Response:

Health Care Providers: The impact of HIPAA requires a single uniform standard on conducting health care transactions so they are not required to create a new proprietary means of transacting electronic business each time they take on a new business partner. These standards will reduce costs, complexity, and confusion.
DHS interfaces with some 12,000-15,000 Providers electronically and another 12,000-15,000 manually.

Clients: Compliance with HIPAA mandates that access to health information is limited to minimally necessary disclosures as required by state law or federal regulation. Protection of the health information is mandated and forbids the information from being sold, traded or otherwise used without the permission and prior consent of the client. Both the privacy and security segments of the HIPAA law ensures every citizen that his or her personal health information (PHI) is not misused.
DHS serves (January 2004) some 1,175,713 clients a year with total annual benefits of $2, 775,613,346.00. This equates to over $3,000.00 per person served (almost $950.00 per person in the State population of 2,926,354. Bottom line, we serve 31% of the state population with 1 or more Plan dollars.
Insurance Companies: The impact of HIPAA creates a single uniform standard on conducting electronic health care transactions so they are not required to create a new proprietary means of transacting electronic business each time they take on a new business partner. The standard will reduce costs, complexity.
NOTE
Going forward during the next several years the following deficiencies must be remedied.
The Gartner assessment compiled the following statistics –
Iowa DHS is spending less than comparison peer groups in the following areas -
- Personnel 52.7% less
- Hardware 28.2% less
- Software 15.7% less
- Outsource 56.1% less
- Transmission 14.4% less
- Occupancy 40.4% less
- Disaster Recovery 100% less

The aggregate IT consensus model costs for Iowa DHS for those modules included in the analysis are 58.1% lower than what the composite peer group would spend to perform IOWA's DHS workload.
DHS Focus going forward with the new IT Strategy Direction for at least the next 3 years -
1. Communication and Alignment of IS / IT to the Business Units
2. Proper Staffing Resources and Skills
3. Distributed Computing
4. Disaster Recovery and Data Security.

Conclusion: Existing IT infrastructure is impacting and hampering business process improvement needs.

c. Citizen Impact

Summarize how the project leads to a more informed citizenry, facilitates accountability, and encourages participatory democracy. If this is an extension of another project, what has been the adopted rate of Iowa's citizens or government employees with the preceding project?
Response:

This ongoing project will over time provide a conduit to securely share data with other agencies and serve as a model methodology and platform for other agencies to follow.
Clients of DHS (numbering 1,175,713) all will have access to their data with a very high degree of security and modern technology.
Proposed Strategy and Environment will
1.will deliver to any Iowan the opportunity to actively participate in the efficient and effective delivery of services entrusted to the department to manage.
2. Eliminate all barriers – wherever they exist – preventing Iowans from obtaining needed services for Health, Safety, Stability, and Self-Sufficiency
3. Remove all obstacles – real and perceived – preventing timely, effective, and efficient service to Iowans in need.

d. Public Health and/or Safety

Explain requirements or impact on the health and safety of the public.
Response:
DHS Mission - is responsible for the administration of the following volume of benefits.
DHS serves (January 2004) some 1,175,713 clients a year with total annual benefits of $2,775,613,346.00. This equates to over $3,000.00 per person served (almost $950.00 per person in the State population of 2,926,354. Bottom line, we serve 31% of the state population with 1 or more Plan dollars.

To help individuals and families achieve safe, stable, self-sufficient, and healthy lives, thereby contributing to the economic growth of the state.

[This section to be scored by application evaluator.]

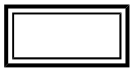
Evaluation (10 Points Maximum)

- Minimally improves Customer Service (0-3 points).
- Moderately improves Customer Service (4-6 points).
- Significantly improves Customer Service (7-10 points).

[This section to be scored by application evaluator.]

Evaluation (15 Points Maximum)

- Minimally directly impacts Iowa citizens (0-5 points).
- Moderately directly impacts Iowa citizens (6-10 points).
- Significantly directly impacts Iowa citizens (11-15 points).



F. Process Reengineering

Provide a pre-project or pre-expenditure (before implementation) description of the impacted system or process. Be sure to include the procedures used to administer the impacted system or process and how citizens interact with the current system.

Response:

The intent of HIPAA Security is to improve all aspects of Confidentiality, Integrity and Availability. The pursuit of Best Business Practices insures continuous life cycle vigilance insuring the continuous effort to sustain changing business processes and practices. This includes emergency operations, disaster recovery, all aspects of configuration management and business continuity.

The organizations affected are all state agencies who process confidential health data, and providers (institutions and private organizations).

Provide a post-project or post-expenditure (after implementation) description of the impacted system or process. Be sure to include the procedures used to administer the impacted system or process and how citizens will interact with the proposed system. In particular, note if the project or expenditure makes use of information technology in reengineering traditional government processes.

Response:

This request represents SFY 2006 funding to continue federal requirements for HIPAA Security and the new DHS IT Strategy Direction. Initial efforts started in SFY 2003; the schedule will look at the next 3 years (through Fiscal ’08).

This funding request supports:

--Project planning and project management required to implement federal requirements.

--Application remediation and system programming.

--Increased tracking for claim payment and release of identifiable health care information

--Gains from improvements in technology

This funding request will produce the following results:
--Complete and accurate federal reporting

--Implementation of HIPAA Security requirements. Failure to comply with HIPAA requirements can result in up to $25,000 per person, annually, with the addition of civil penalties. See Opportunity Value/Risk or Loss Avoidance Benefit for full penalty clauses.

The 6 primary initial system targets are IABC, Title 19, STAR, ICAR, FACSM, MMIS.
These very large legacy mainframe systems have been targeted by Gartner and DHS for replacement. The approach is to develop component parts in free standing modules in new technologies. Eventually the legacy systems would be phased out and replaced by new supporting modules. The development will be dependent on a well thought out approach to enhancements surrounding the alignment to Business direction.

-- The following Gartner Future System Capabilities requirements will be addressed over time system by system –
1. Ability to address complex/multiple relationships
2. Multi-channel management and call center
3. Workflow Management
4. Intelligent Scripting
5. Modularity of applications for multiple programs
6. Ease of maintenance and upgrade
7. System Administration by business representatives, not technology
8. Program Interfaces
9. Multi-level access control
10. Automated reporting and program analytics.

Provide a post-project or post-expenditure (after implementation) description of the impacted system or process. Be sure to include the procedures used to administer the impacted system or process and how citizens will interact with the proposed system. In particular, note if the project or expenditure makes use of information technology in reengineering traditional government processes.
Response:
This request represents SFY 2006 funding to continue federal requirements for HIPAA Security and the new DHS IT Strategy Direction. Initial efforts started in SFY 2003; the schedule will look at the next 3 years (through Fiscal ’08).

This funding request supports:

--Project planning and project management required to implement federal requirements.

--Application remediation and system programming.

--Increased tracking for claim payment and release of identifiable health care information

--Gains from improvements in technology

This funding request will produce the following results:
--Complete and accurate federal reporting

--Implementation of HIPAA Security requirements. Failure to comply with HIPAA requirements can result in up to $25,000 per person, annually, with the addition of civil penalties. See Opportunity Value/Risk or Loss Avoidance Benefit for full penalty clauses.

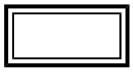
The 6 primary initial system targets are IABC, Title 19, STAR, ICAR, FACSM, MMIS.
These very large legacy mainframe systems have been targeted by Gartner and DHS for replacement. The approach is to develop component parts in free standing modules in new technologies. Eventually the legacy systems would be phased out and replaced by new supporting modules. The development will be dependent on a well thought out approach to enhancements surrounding the alignment to Business direction.

-- The following Gartner Future System Capabilities requirements will be addressed over time system by system –
1. Ability to address complex/multiple relationships
2. Multi-channel management and call center
3. Workflow Management
4. Intelligent Scripting
5. Modularity of applications for multiple programs
6. Ease of maintenance and upgrade
7. System Administration by business representatives, not technology
8. Program Interfaces
9. Multi-level access control
10. Automated reporting and program analytics.

[This section to be scored by application evaluator.]

Evaluation (10 Points Maximum)

- Minimal use of information technology to reengineer government processes (0-3 points).
- Moderate use of information technology to reengineer government processes (4-6 points).
- Significant use of information technology to reengineer government processes (7-10).



G. Timeline

Provide a projected timeline for this project. Include such items as planning, database design, coding, implementation, testing, conversion, parallel installation, and date of final release. Also include the parties responsible for each item.

Response:

[This section to be scored by application evaluator.]

Evaluation (5 Points Maximum)

- The timeline contains several problem areas (0-2 points)
- The timeline seems reasonable with few problem areas (3-4 points)
- The timeline seems reasonable with no problem areas (5)

H. Funding Requirements

On a fiscal year basis, enter the estimated cost by funding source: Be sure to include developmental costs and ongoing costs, such as those for hosting the site, maintenance, upgrades, ...

	FY06		FY07		FY08	
	Cost($)	% Total Cost	Cost ($)	% Total Cost	Cost ($)	% Total Cost
State General Fund	$54,400	4%	$0	0%	$0	0%
Pooled Tech. Fund /IowAccess Fund	$750,000	61%	$0	0%	$0	0%
Federal Funds	$421,875	34%	$0	0%	$0	0%
Local Gov. Funds	$0	0%	$0	0%	$0	0%
Grant or Private Funds	$0	0%	$0	0%	$0	0%
Other Funds (Specify)	$0	0%	$0	0%	$0	0%
Total Project Cost	$1,226,275	100%	$0	100%	$0	100%
Non-Pooled Tech. Total	$476,275	39%	$0	0%	$0	0%

[This section to be scored by application evaluator.]

Evaluation (10 Points Maximum)

- The funding request contains questionable items (0-3 points)
- The funding request seems reasonable with few questionable items (4-6 points)
- The funding request seems reasonable with no problem areas (7-10)

I. Scope

Is this project the first part of a future, larger project?

☑ YES (If "YES", explain.) ☐ NO, it is a stand-alone project.

Explanation:

While ’05 is a continuation of efforts starting with HIPAA in 2000 HIPAA and Gartner analysis in ’04 has led to progressive NEXT STEPS outlined above. The strategic plan being developed will cover 3 years, will be very large in scope and will take several years to complete, particularly major legacy system renovation / rewrites

Is this project a continuation of a previously begun project?

☑ YES (If "YES", explain.)

Explanation:

HIPAA kicked off initial efforts in 2000 and we have aggressively pursued compliance during 02, 03, 04. Transactions and codes sets are implemented and Privacy is nearing completion. Ground work for Security was laid during ’04 and continues into ’05 along with the new IT Strategy Direction under development by an IT Executive Oversight Group plans are being developed for the next 3 years knowing it will extend to ’08 and beyond.

Funding in ’02-‘03 was $2,100,00, Tobacco Funds. ’03-’04 was $322,874.00 Pooled Tech and $1,398,600 in General Admin. ’04-’05 brings $684,254.00 in Pooled Tech.

J. Source of Funds

On a fiscal year basis, how much of the total project cost ($ amount and %) would be absorbed by your agency from non-Pooled Technology and/or IOWAccess funds? If desired, provide additional comment / response below.

Response:

In previous years personnel time (from as high as 80 persons) was absorbed but there are no metrics to know how many $ was truly absorbed by the agency. In ‘03’04 we had a very unusual situation where in fiscal management was able to contribute $1,398,600. In fiscal ’04 DHS will absorb only a known figure of approximately $54,400 (2 ½ time FTE’s) but again with involvement of dozens of personnel cost absorption is not being captured.

Typically new ongoing costs of supporting new initiatives is absorbed back into the organization thus no ongoing costs.

[This section to be scored by application evaluator.]

Evaluation (5 Points Maximum)

- 0% (0 points)
- 1%-12% (1 point)
- 13%-25% (2 points)
- 25%-38% (3 points)
- 39%-50% (4 points)
- Over 50% (5 points)

Section II: Financial Analysis

A. Project Budget Table

It is necessary to estimate and assign a useful life figure to each cost identified in the project budget. Useful life is the amount of time that project related equipment, products, or services are utilized before they are updated or replaced. In general, the useful life of hardware is three (3) years and the useful life of software is four (4) years. Depending upon the nature of the expense, the useful life for other project costs will vary between one (1) and four (4) years. On an exception basis, the useful life of individual project elements or the project as a whole may exceed four (4) years. Additionally, the ROI calculation must include all new annual ongoing costs that are project related.

The Total Annual Prorated Cost (State Share) will be calculated based on the following equation:

$$\left[\left(\frac{Budget\ Amount}{Useful\ Life}\right) \times \%\ State\ Share\right] + \left(Annual\ Ongoing\ Cost \times \%\ State\ Share\right) = Annual\ Prorated\ Cost$$

Budget Line Items	Budget Amount (1st Year Cost)	Useful Life (Years)	% State Share	Annual Ongoing Cost (After 1st Year)	% State Share	Annual Prorated Cost
Agency Staff	$54,400	1	64.00%	$0	0.00%	$34,816
Software	$234,375	4	64.00%	$0	0.00%	$37,500
Hardware	$100,000	3	64.00%	$0	0.00%	$21,333
Training	$50,000	4	64.00%	$0	0.00%	$8,000
Facilities	$0	1	64.00%	$0	0.00%	$0
Professional Services	$682,500	4	64.00%	$0	0.00%	$109,200
ITD Services	$0	4	0.00%	$0	0.00%	$0
Supplies, Maint, etc.	$5,000	1	64.00%	$0	0.00%	$3,200
Other	$100,000	1	64.00%	$0	0.00%	$64,000
Totals	$1,226,275	---	---	$0	---	$278,049

B. Spending Plan

Explain how the funds will be allocated.

Response:

Software and hardware expense will be used to harden network vulnerabilities with intrusion detection automated software. Professional services will be used for a variety of purposes, project management, ITIL-ITSM DEVELOPMENT, mainframe programming, Business Continuity audits and testing, professional security consulting. Ongoing costs (none reflected in above table) are absorbed into the organization UNLESS funds become available to support specific costs. Whether legislative requirements or otherwise Policy and IT areas of DHS take on the added burden, i.e., new policies and procedures, new tools to support, etc.

C. Tangible and/or Intangible Benefits

Respond to the following and transfer data to the ROI Financial Worksheet as necessary:

1. Annual Pre-Project Cost - This section should be completed only if state government operations costs are expected to be reduced as a result of project implementation. **Quantify actual state government direct and indirect costs** (personnel, support, equipment, etc.) associated with the activity, system or process prior to project implementation.
Describe Annual Pre-Project Cost:

Quantify Annual Pre-Project Cost:

	State Total
FTE Cost (salary plus benefits):	$0.00
Support Cost (i.e. office supplies, telephone, pagers, travel, etc.):	$0.00
Other Cost (expense items other than FTEs & support costs, i.e. indirect costs if applicable, etc.):	$0.00
Total Annual Pre-Project Cost:	$0.00

2. Annual Post-Project Cost - This section should be completed only if state government operations costs are expected to be reduced as a result of project implementation. **Quantify actual state government direct and indirect costs** (personnel, support, equipment, etc.) associated with the activity, system or process after project implementation.
Describe Annual Post-Project Cost:

Quantify Annual Post-Project Cost:

	State Total
FTE Cost (salary plus benefits):	$0.00
Support Cost (i.e. office supplies, telephone, pagers, travel, etc.):	$0.00
Other Cost (expense items other than FTEs & support costs, i.e. indirect costs if applicable, etc.):	$0.00
Total Annual Post-Project Cost:	$0.00

3. Citizen Benefit - Quantify the estimated annual value of the project to Iowa citizens. This includes the "hard cost" value of avoiding expenses ("hidden taxes") related to conducting business with State government. These expenses may be of a personal or business nature. They could be related to transportation, the time expended on or waiting for the manual processing of governmental paperwork such as licenses or applications, taking time off work, mailing, or other similar expenses. As a "rule of thumb," use a value of $10 per hour for citizen time.

Describe savings justification:

Transaction Savings

Number of annual online transactions:	0
Hours saved/transaction:	0
Number of Citizens affected:	0
Value of Citizen Hour	0
Total Transaction Savings:	$0
Other Savings (Describe)	$0
Total Savings:	$0

4. Opportunity Value/Risk or Loss avoidance - Quantify the estimated annual non-operations benefit to State government. This could include such items as qualifying for additional matching funds, avoiding the loss of matching funds, avoiding program penalties/sanctions or interest charges, avoiding risks to health/security/safety, avoiding the consequences of not complying with State or Federal laws, providing enhanced services, avoiding the consequences of not complying with enterprise technology standards, etc.

Response:
1.Potential Sanctions / fines are a minimum of 6,650,000,000. This would be the fine to DHS as a covered entity applicable to Medicaid alone. We do not have an estimate of the rest of DHS Health Care Components. Section 1176 of the Act establishes civil monetary penalties for violation of the provisions in part C of title XI of the Act, subject to several limitations. Penalties may not be more than $100 per person per violation of a provision and not more than $25,000 per person per violation of an identical requirement or prohibition for a calendar year. With certain exceptions, the procedural provisions in section 1128A of the Act, "Civil Monetary Penalties," are applicable to imposition of these penalties. Section 1177 of the Act established penalties for any person that knowingly misuses a unique health identifier, or obtains or discloses individually identifiable health information in violation of this part. The penalties include: (1) A find of not more than $50,000 and/or imprisonment of not more than 1 year; (2) if the offense is "under false pretenses" a fine of not more than $100,000 and /or imprisonment of not more the 5 years; and (3) if the offense is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than $250,000 and/or imprisonment of not more than 10 years. We note that these penalties do not affect any other penalties that may be imposed by other federal programs.

2. The opportunity to leverage State dollars by obtaining 36% Federal Match.
3. The opportunity to keep Medicaid Systems certified for 90% Federal match for systems development and implementation.

5. Benefits Not Readily Quantifiable - List and summarize the overall non-quantifiable benefits (i.e., IT innovation, unique system application, utilization of new technology, hidden taxes, improving the quality of life, reducing the government hassle factor, meeting a strategic goal, etc.).

Response:

1. Improved Systems and IT alignment with business requirements.
2. Benefits of best practices impact on business models
3. Benefits of enterprise thinking
4. Posture to proactively support changing business requirements
5. Posture to proactively maintain and support $2.776 Billion in client benefits.
6. Posture to recover for emergency operations, disaster.
7.The opportunity to pilot ITIL-ITSM as a departmental and possibly an enterprise model.
8. The opportunity to deliver on the DHS IT Strategy Direction.
9. The opportunity of better leveraging state dollars and matching federal funds.
11.The opportunity to maintain a low per capita cost which is 8%
below peer groups.
12. Full compliance with Federal requirement and think-tank methodology

ROI Financial Worksheet	
A. Total Annual Pre-Project cost (State Share from Section II C1):	$0
B. Total Annual Post-Project cost (State Share from Section II C2):	$0
State Government Benefit (= A-B):	$0
Annual Benefit Summary:	$0
State Government Benefit:	$0
Citizen Benefit:	$0
Opportunity Value or Risk/Loss Avoidance Benefit:	$6,650,000,000
C. Total Annual Project Benefit:	$6,650,000,000
D. Annual Prorated Cost (From Budget Table):	$278,049
Benefit / Cost Ratio: (C/D) =	23,916.62
Return On Investment (ROI): ((C-D) / Requested Project Funds) * 100 =	886,629.59%

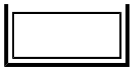
[This section to be scored by application evaluator.]

Evaluation (25 Points Maximum)

- The financial analysis contains several questionable entries and provides minimal financial benefit to citizens (0-8 points).
- The financial analysis seems reasonable with few questionable entries and provides a

moderate financial benefit to citizens (9-16 points).

- The financial analysis seems reasonable with no problem areas and provides maximum financial benefit to citizens (17-25).



Note: For projects where no State Government Benefit, Citizen Benefit, or Opportunity Value or Risk/Loss Avoidance Benefit is created due to the nature of the project, the Benefit/Cost Ratio and Return on Investment values are set to Zero.

Appendix A. Auditable Outcome Measures

For each of the following categories, list the auditable metrics for success after implementation and identify how they will be measured.

1. Improved customer service

a. Service Level Agreement (SLA) monitoring metrics from ITIL-ITSM and Remedy-Magic SLA reporting stats
b. IT investment management metrics derived from ITIL-ITSM and Remedy-Magic Investment Management Asset Module.

c. Incident Management metrics from ITIL-ITSM model and Remedy- Magic Incident Management Module.
d. Configuration Management metrics from ITIL-ITSM and Remedy-Magic configuration management module

2. Citizen impact

Stable or decreasing per capita costs and far greater access to state services

3. Cost Savings

Indeterminable at this early juncture in planning. But prior experience and Gartner expectations through CMM alone would be very substantial. Its the intangible benefits to a 1,000,000 + client base which is expected to be the most obvious benefit along with the department being in a proactive mode to the changing needs of its business units.

4. Project reengineering

All major legacy mainframe applications will rise to modern modular technology over the timeframe outlined in the Strategic Plan currently under development

5. Source of funds (Budget %)

There are no envisioned funds beyond this request despite the fact that we continue to look for possibilities of grants.

6. Tangible/Intangible benefits

Return